REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	22 May 03	SAMS Monograph 17 Jul02-22May 03

4. TITLE AND SUBTITLE
Educating Officers in Information Operations: Is the U.S. Army Moving in the Right Direction?

5. FUNDING NUMBERS

6. AUTHOR(S)
LTC Thomas R. Gregory

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
1 Reynolds Ave
Ft. Leavenworth, KS 66027

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release: distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 words)* see attached

14. SUBJECT TERMS

15. NUMBER OF PAGES
48

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Educating Officers in Information Operations: Is the U.S. Army Moving in the Right Direction?

A Monograph
by
LTC Thomas R. Gregory
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas
First Term AY 00-01

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

LTC Thomas R. Gregory

Title of Monograph: Educating Officers in Information Operations: Is the U.S. Army moving in the right direction?

Approved by:

_____	Monograph Director
Peter J. Schifferle, Ph.D.	
_____	Professor and Director Academic Affairs, School of Advanced Military Studies
Robert H. Berlin, Ph.D.	
_____	Director, Graduate Degree Program
Philip J. Brookes, Ph.D.	

Abstract

EDUCATING OFFICERS IN INFORMATION OPERATIONS: IS THE U.S. ARMY MOVING IN THE RIGHT DIRECTION? by LTC Thomas R. Gregory, U.S. Army 45 pages.

Information Operations are becoming increasingly important in military operations. While many of the components that comprise Information Operations are not new the U.S. Army is attempting to better synchronize these components to increase their battlefield effects. To accomplish this aim the Army has produced new doctrine for Information Operations and even created a new career field for commissioned officers (FA30) to address Information Operations.

This study examines the doctrine that exists to support Information Operations as well as how Information Operations is being incorporated into the Army's Officer Education System. The study begins by describing a current military operation where Information Operations was the main effort. This case study selected was an operation conducted in Bosnia Herzegovina titled, "Operation Bosanova". The study next analyzes current and future U.S. Army doctrine for Information Operations. Next, the study addresses how Information Operations are taught as part of the current Officer Education System. The study concludes with a series of recommendations for how Information Operations should be taught as part of the Officer Education System.

The conclusion of the study is that while sufficient doctrine currently exists within the U.S. Army to conduct Information Operations, there is an Army wide lack of any education in the discipline. While a concerted effort is being made to ensure that the Army has trained FA30 officers, no real training exists for the remainder of the officer corps to become educated in the fundamentals of Information Operations. It is this lack Information Operations education for all officers that is the biggest identified weakness of this study

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

Information Operations are becoming an area of ever increasing importance in modern military operations. It is imperative that that U.S. Army includes instruction on Information Operations in its Officer Education System.

> How we respond to dynamic changes concerning potential adversaries, technological advances and their implications, and the emerging importance of information superiority will dramatically impact how well our Armed Forces can perform its duties in 2010.[1]

This statement by the then Chairman of the Joint Chiefs of Staff, General John Shalikashvili, introduced the United States (U.S.) Armed Forces to the world of Information Age Warfare. Since this document was published all branches of the U.S. military have begun to develop doctrine, training and education to support Information Operations. More than five million hits are received by simply typing the term Information Operations into an Internet search engine. The U.S. Army regarded Information Operations to be of such importance that they created a new career field for Commissioned Officers as part of OPMS XXI; Functional Area 30 Information Operations. Regardless of the emphasis being put on Information Operations, it remains a "buzz word" for most commanders and their staffs in the U.S. Army. It is a topic that seems to have a different meaning for every person you ask. One commander may view it as primarily a "Signal Corps thing"; in his view it's all about computers and automation. Another commander sees Information

[1] Department of Defense, Chairman of the Joint Chiefs of Staff, *Joint Vision 2010* (Washington D.C.: U.S. Government Printing Office, 1996) p.8.

Operations as an increased emphasis on Public Affairs. While these are in fact part of Information Operations they are just that, only part of it.

The confusion about Information Operations is not limited to the U.S. Army. While Information Operations is a Joint concept, each individual service has a unique and different interpretation of it.[2] The U.S. Navy sees Information Operations primarily as the ability to more efficiently link sensors to shooters. The U.S. Air Force is trying to become the Information Operations service of choice for the Department of Defense and sees a natural link between their preeminent role in the control of U.S. military space assets and cyber security. The U.S. Army views Information Operations as the commander's ability to mass the effects of the information element of combat power.[3] It is this confusion, or lack of common understanding, that is the genesis for this monograph. Before Information Operations can be defined or applied to the Army's military operations, the basic principals must first be agreed upon by the sister services in the Department of Defense. This paper will touch on the Joint and sister service issues only where they apply; the primary focus will be on current U.S. Army doctrine as well as the current system for educating officers in Information Operations. The premise of this paper is that there is a significant weakness in the way that Information Operations is taught throughout the U.S. Army's Officer Education System (OES).

The first step creates an understanding of what Information Operations is, and identifies the basic common knowledge required by defining the current U.S. Army

---

[2]David S. Alberts, John J. Garska, and Frederick P. Stein, *Network Centric Warfare* (Command and Control Research Program, 2002). The authors idea that each service has a different view of what Information Operations is was derived from reading this book.

[3] Department of the Army, FM 3-13 *(DRAG) Information Operations* (Washington D.C.: Office of the Chief of Staff of the Army, Draft 2002) p 1-1.

doctrine for Information Operations. An assessment is made to determine if the current Army Information Operations Doctrine is sufficient to create a strong understanding of the subject, or if the doctrine is insufficient and therefore part of the problem. The current FM 100-6 *Information Operations* Army Field Manual, the new FM 3-13 *Information Operations* (DRAG) (which is in final coordinating draft) and the FM 3.0 *Operations* manual is used as the primary Army manuals for this assessment. This monograph addresses Joint Publication 3-13 *Information Operations* to ensure that Army doctrine is consistent with the published joint doctrine.

The second step assesses how Information Operations is taught as part of the current OES, to include FA 30 officers as well as all U.S. Army officers, regardless of branch. This paper identifies how Information Operations is addressed in the Officer Advanced Courses, Combined Arms Services Staff School (CAS3), U.S. Army Command and General Staff College (CGSC) Advanced Military Studies Program (AMSP) and the Army War College. This includes the current training/education, as well as the proposed training/education under the new Intermediate Level Education (ILE) program. This paper also determines whether the current system is educating officers with a thorough understanding of Information Operations, and identifies any deficiencies.

The third step describes a recent military operation where Information Operations were extensively used. The intent is to show the value Information Operations has in contemporary military operations and describe how the Information Operations were planned and executed.

Finally, a solution is put forth as to how Information Operations should be taught for both basic branch officers as well as FA30 officers. Each school's current Program

of Instruction is used to create a baseline, followed by an overall assessment to identify where the Army currently is in their education of officers in the field of Information Operations, and where they need to go in the future.

CHAPTER TWO

"Operation Bosanova"

A recent military operation in Bosnia Herzegovina (BH) involving the seizure of a television station designated "Operation Bosanova" highlights the effectiveness of U.S. Army Information Operations doctrine and education/training when applied to a military operation. The reason for choosing this operation is twofold: First, the U.S. Army has been involved in military operations in BH since 1994, making this commitment of forces a mature theater to study. Secondly, since the Commander at the Stabilization Force (SFOR) was a U.S. Army General Officer, and the Information Operations planning cell primarily staffed with U.S. personnel, this operation is a good example of the application of U.S. Army Information Operations doctrine and training. This operation demonstrates the effectiveness of applying Information Operations principals during mission analysis and course of action development making this scenario relevant for analysis. SFOR after action reviews (AARs) conducted and documented at the conclusion of the operation will be used to detail this operation.[4]

Operation Bosanova was conducted by SFOR in October of 1999 to stop the transmission of anti Dayton Peace Accords and anti SFOR rhetoric being transmitted from a particular television station in BH.

The Commander SFOR (COMSFOR) determined that this rhetoric from the Serb television station was becoming detrimental to the mission of SFOR and had the potential to inflame already existing tensions in BH. He directed his staff to develop a plan to stop

[4] "Operation Bosanova" AAR's are controlled by the SFOR Command Historians Office and only accessible by personnel with access to the NATO SFOR Local Area Network

this television station from broadcasting and to determine the best way to take the station off the air while making sure that it was accomplished in a manner that did not make SFOR appear to be repressive. The mission of forces in BH was to promote peace and move the country to democratic principles, not to become the new repressor of rights in BH. This mission had to be accomplished with this goal in mind.

The planning cell at SFOR came up with four Information Operations related considerations that guided them through the process of developing their plan for Operation Bosanova.[5] These considerations can be framed into four questions: 1) Are we targeting radio or television, both or other media? 2) Do we want to jam transmissions, close them down, or open up media traffic? 3) Do we want to open (or close) just one faction, or the entire network? 4) We will certainly want to target nodes of some sort, but can we choose key sites away from populated areas to avoid confrontation with armed factions and/or large crowds?

The SFOR cell first addressed the question of which media to target. Since only one television station was broadcasting inflammatory information, the decision was made to limit the target to that one station. This ensured that SFOR was not seen as trying to stifle all opinions in BH, rather to target the offending inflammatory information source. Keeping media sources open was a key consideration in the decision to shut down only the offending station.

Next, the decision had to be made as to how to shut them down. There were several options available to SFOR to accomplish this task; the television signal could be

[5] Information for this section was accessed from the COMSFOR LAN (Operation Bosanova AAR) during an operational deployment by the author to Bosnia Herzegovina during January of 2003.

jammed or the station could be taken off the air with the use of force. In order to jam the television broadcast, the COMSFOR had at his disposal the U.S. Air Force EC 130 Commando Solo that can jam a number of radio frequencies. This option was rejected because it would have committed a valuable asset that could be better used to accomplish other, more important tasks. The cell decided that the use of force was the most efficient way of taking the station off the air and would provide a more permanent solution to the problem at hand. By taking physical control of the station, it could be kept on the air and used to advantage by shaping opinions with a pro SFOR and pro Dayton message.

The final consideration was exactly how to target the television station in a way that could best accomplish all of SFOR's requirements. Since a decision was made to use the station to further the IO campaign, physical destruction was eliminated as an option. Another consideration was to avoid large civilian demonstrations during the execution of the mission. This led to a plan that bypassed the most obvious course of action, which was occupying the television studio directly. Instead of trying to occupy the studio in a heavily populated area, the decision was made to take physical control of the remote transmission sites; this would take the offending station off the air. These sites were located in very sparsely populated areas and would accomplish the mission of turning off the television broadcasts. Without these remote transmission sites, the television studio was rendered inoperative and could not broadcast its offending messages. It also saved the infrastructure so that SFOR could take control of the main studio at a later date and reactivate the station once a more acceptable message was ready to be sent.[6]

[6] Information accessed from the COMSFOR LAN (Operation Bosanova AAR) during an operational deployment by the author to Bosnia Herzegovina during January of 2003.

Overall "Operation Bosanova" was a total success for the COMSFOR. The reason for including it as a case study is to show how Information Operations has become an integral part of military operations in the 21st century. "Operation Bosanova" demonstrates how not only are commanders and staffs being required to included Information Operations as a key supporting element to military operations, but how they can also be the main effort in some military operations.

CHAPTER THREE

Current United States Army Information Operations Doctrine

After the publication of *Joint Vision 2010*, published in 1996, the Army was the first service to try and capture the idea of Information Operations in a doctrinal manual. The U.S. Army Training and Doctrine Command (TRADOC) published TRADOC Pamphlet 525-5, *Force XXI Operations*, to establish a framework for the Army to use to begin considering Information Operations in its operations.[7] This publication was followed by FM 100-6, *Information Operations*, which was published in 1996. With the publication of FM 100-6, the Army became the first service to try and capture the concept of Information Operations and establish a framework to incorporate these concepts into Army operations. While initially this publication was looked at by the field as a revolutionary manual, this perception proved to be incorrect.

FM 100-6 *Information Operations* established three specific areas to what the Army identified as Information Operations: Civil Affairs, Public Affairs and Command and Control Warfare.[8] While the term Information Operations was new, none of these concepts were, and in fact had been included in military operations for a long period of time. The Chinese military theorist Sun Tzu around 400BC spoke of shaping the enemy's perception of the world to manipulate his plans and actions.[9] The only difference was that now these individual operations had been grouped together with more importance attached to them. With the advent of the increased reliance on technology in the Armed

---

[7] TRADOC PAM 525-5, Force XXI Operations, 1 August 1994

[8] Charles N. Eassa, US Armed Forces Information Operations-Is the Doctrine Adequate. School of Advanced Military Studies, USACGSC, Fort Leavenworth, Ks. First Term AY 99-00.

[9] Sun Tzu, The Art of War (New York: Oxford University Press, 1996)

Forces, these previously disparate operations now needed to be controlled and synchronized under the moniker of Information Operations.

FM 100-6 *Information Operations* did an excellent job of defining the overall concept of Information Operations providing detail in describing the "Information Environment" that now exists due to the increased dependency of our armed forces on technology. It also described how the areas of Civil Affairs, Public Affairs and Command and Control Warfare needed to be more closely integrated. While it was effective in identifying large concepts, it was weak in the actual planning and execution phases of Information Operations. The doctrine failed to specify who was responsible for a specific activity at specific level and what payoffs could be expected, making it difficult for tactical commanders to visualize. Since there was virtually no Information Operations experience or resources provided, the doctrine was left to local interpretation and integration.[10]

As an observer trainer at the Battle Command Training Program from 1996 until 1998 the author witnessed this confusion first hand. Each headquarters we evaluated handled the integration of Information Operations in a different way; one headquarters would assign IO to the G6 while another would place the responsibility with either the G3 or the G5. With no doctrinal guidance on where Information Operations responsibility should rest each command assigned the responsibility for Information Operations as they saw fit.[11]

---

[10] Charles N. Eassa, US Armed Forces Information Operations-Is the Doctrine Adequate. School of Advanced Military Studies, USACGSC, Fort Leavenworth, Ks. First Term AY 99-00.

[11] This author while assigned to Team Delta of the Battle Command Training Program (BCTP) as an observer Trainer from July 1996 to July 1998. He was assigned to the Command and Control Operating System and specifically worked on Signal and Information Operations issues for the team.

Another weakness with FM 100-6 *Information Operations* is that it was published prior to the Joint Doctrine on Information Operations. While the Army published its document in 1996, it was not until 1998 that Joint Pub 3-13 *Information Operations* was published. With this disparity in the publication dates, it is obvious why Army doctrine and Joint Doctrine do not even use the same definition of Information Operations.

FM 100-6 defines Information Operations as:

> Information Operations integrate all aspects of information to accomplish the full potential for enhancing the conduct of military operations. Information operations are not new. In their simplest form they are the activities that gain information and knowledge and improve friendly execution of operations while denying an adversary similar capabilities by whatever possible means. Effects of IO produce significant military advantage for forces conducting such operations.[12]

Joint Publication 3-13 defines Information Operations as:

> Information Operations (IO) involves actions taken to affect adversary information and information systems while defending one's own information and information systems. They apply across all phases of an operation, the range of military operations, and every level of war.[13]

It is understandable why these definitions are not nested; however the Army's neglect in bringing its doctrine in line with the Joint Doctrine even after more than four years is unsettling. FM 3-13 *Information Operations* (DRAG) is the Army's second iteration of doctrine for Information Operations, which should finally rectify this problem.

---

[12] Department of the Army, FM 100-6 *Information Operations* (Washington D.C.: Office of the Chief of Staff of the Army, 1996).

[13] Joint Publication 3-13, *Joint Doctrine for Information Operations*, Washington D.C., JCS, 1998.

FM 3-13 *Information Operations* (DRAG) is a drastic improvement over FM 100-6 *Information Operations*. It not only clearly defines the "Information Environment", it also lays out numerous Tactics, Techniques and Procedures (TTP) for conducting Information Operations. FM 3-13 *Information Operations* addresses these TTPs in numerous scenarios across the range of military operations. The inclusion of these TTPs gives commanders and staffs an idea of what right looks like when it comes to conducting Information Operations. The new field manual also includes a series of matrices that show each element of Information Operations along with a list of possible events that could be executed for each element. In addition, detailed examples of Information Operations considerations throughout the Military Decision-Making Process (MDMP) are identified along with an example of what an Information Operations Annex could look like.

While all of these are improvements to FM 100-6, the biggest improvement is how the publication assigns Information Operations responsibility within the staff. Initially FM 3-13 directed the creation of a new staff section, the G7, to support Information Operations planning in which the Officer in Charge (OIC) would work directly for the Chief of Staff. This is currently being removed from the document, and the Information Operations section will then be designated for inclusion into the existing G3 structure of the staff.[14]

FM 3.0 *Operations* is the Army's capstone operations doctrine that describes how Army forces, as part of a joint team, will be responsive and dominant across the full

[14] The author received this information during a discussion of *FM 3-13 Information Operations* with several members of the Information Operations proponency office at Fort Leavenworth, Kansas in November of 2002.

spectrum of operations.[15] An entire chapter is dedicated to the subject of Information Superiority, identifying Information Operations as one of three key tenets necessary to achieve Information Superiority on the modern battlefield. It describes an environment where Information Operations, coupled with Information Management and Intelligence, Surveillance and Reconnaissance (ISR) are integrated, resulting in relevant information being available to the commander in the field, allowing him to gain an operational advantage over his opponent.[16] FM 3.0 describes Information Operations as shaping operations that create and preserve opportunities for decisive operations. It is through the integrated application of the twelve elements of both offensive and defensive IO that the environment is shaped. Per Chapter 11 of FM 3.0 these elements of Information Operations are: Military Deception, Counterdeception, Operations Security (OPSEC), Physical Security, Electronic Warfare, Information Assurance, Physical Destruction, Psychological Operations (PSYOP), Counterpropaganda, Counterintelligence, Computer Network Attack and Computer Network Defense.

This publication also identifies two related activities that contribute to Army Information Operations: Public Affairs and Civil Military Operations. These are important because they communicate information to activities critical audiences to influence their understanding and perception of military operations.[17]

---

[15] Department of the Army, FM 3.0. *Operations*, (Washington , D.C. Government Printing Office [GPO] 14 June 2001), Foreword.

[16] Department of the Army, FM 3.0. *Operations*, (Washington , D.C. Government Printing Office [GPO] 14 June 2001), 11-6.

[17] Department of the Army, FM 3.0. *Operations*, (Washington , D.C. Government Printing Office [GPO] 14 June 2001), 1-105.

The appendix to this monograph lists a detailed definition of each of the elements of Information Operations as well as definitions of the two key related activities. One issue that comes to light while reviewing these elements and their related activities of Information Operations is that many of them are not new concepts. With the exception of Information Assurance (IA), Computer Network Attack (CNA) and Computer Network Defense (CND), the other elements and related activities have been present in military operations for over one hundred years.

If Information Operations is already a consideration in planning for and executing modern military operations, why create new doctrine for something that already exists and then create an entire commissioned officer career field to deal with it? The answer is two fold: First, the rapid increase in emphasis on automation and digitization within our military has made the protection of our command and control systems more important than ever. Second is the realization that the informational elements of warfare are becoming more important as we move into a more technologically based world.

The current strength of Information Operations within the Army is in the area of doctrine. The two key Field Manuals that the Army has for planning and conducting Information Operations are FM 3.0 *Operations* and FM 3-13 *Information Operations (DRAG).* Both of these manuals provide the focus that is needed to ensure Information Operations are included in future military operations as well as how that integration is done.

The only issue with the current doctrine for Information Operations is in the timing of the release of the doctrine. As stated earlier, the Army was the first component of the Department of Defense to publish doctrine with FM 100-6 *Information Operations.*

This was then followed several years later with the publication of Joint Pub 3-13 *Information Operations*. The Army is in the process of finalizing their new doctrinal publication FM 3-13 *Information Operations*; the intent here is to bring Army doctrine in line with Joint Doctrine. The problem is that once the new Army doctrine is published the Joint community will begin rewriting Joint Pub on Information operations. It is this constant uncoordinated publication of doctrine that is the only real issue the author can identify in this area. Until it is synchronized across all of DoD each of the services will be constantly rewriting doctrine and the doctrine across DoD will never be synchronized.

CHAPTER FOUR

Current Information Operations Training/Education

There are inconsistencies in the current training / education for U.S. Army officers in the field of Information Operations. These inconsistencies are reflected in the lack of specific Information Operations related instruction at all levels from the Captains Career course through the Army War College.

The first school within the Army's Officer Education System (OES) that included Information Operations within its curriculum was the Combined Arms and Services Staff School (CAS3). In 1998 CAS3 became Phase II of the Captains career course. This meant that all Captains would have to attend both their branch specific advanced course and CAS3 to complete the Captains career course.

Beginning in 1998, and continuing until 2001, CAS3 included an Information Operations block in its curriculum.[18] The Information Operations block was taught as part of a larger exercise, F646 an Army Corps level tactical exercise that was part of the CAS3 curriculum[19]. During this exercise the students had to develop a series of staff estimates for a fictitious combat operation. The estimates produced by each staff group included an Intelligence Estimate, a Logistics Estimate and an Information Operations Estimate. For the Information Operations Estimate each member of the staff group, usually eleven to fourteen Captains, would be assigned a position of a Corps or Division staff officer identified in FM 100-6 as a member of the Information Operations working

[18] The author was a CAS3 instructor from 1998-2000; he instructed 12 total CAS3 classes and taught during the class where the Information Operations block of instruction was first included into the curriculum.

[19] CAS3 Lesson F646 Corps and Division Operations, Ft. Leavenworth, Ks. 1998.

group.[20] Each of the Captains were tasked to develop Information Operations related criteria within his or her assigned specialty that would be compiled to assist with a recommendation on which course of action was most supportable from an Information Operations perspective. The goal of this block of instruction was not to make each officer an expert in Information Operations; it was a general overview that allowed students to gain a basic understanding of Information Operations and its components.

After being a part of the curriculum for three years, this Information Operations block was cut when CAS3 reduced its class days to twenty-five. Currently, the CAS3 curriculum does not include any instruction on Information Operations. This is a drastic change to the CAS3 curriculum from only three years ago. As CAS3 again revamps its current curriculum there is a desire from the current instructors to include a block of instruction on Information Operations within the course.[21]

The United States Army Command and General Staff Officers Course (CGSOC) also include Information Operations as part of its curriculum. Currently, the total time allocated to Information Operations subject material within the basic core CGSOC curriculum is one hour.[22] This one-hour block of instruction is entitled "Information Operations, Joint Force Capabilities", and is taught as a part of the Joint Operations overview. The Department of Joint Military Operations (DJMO) teaches it to all students who attend CGSOC. The only other Information Operations related instruction included

---

[20] Department of the Army, FM 100-6 *Information Operations* (Washington D.C.: Office of the Chief of Staff of the Army, 1996) p 6-2

[21] Interview with current CAS3 instructor MAJ (P) Joe Layton conducted at Ft. Leavenworth, Ks. February 2003.

[22] Interview conducted with LtCol Rich Snyder, Information Operations Instructor for United States Army Command & General Staff College, Ft. Leavenworth, Kansas. Conducted in February 2003.

for all students of the Command and General Staff College are two classes that deal with the subjects of Operational Protection and Operations Security and Deception. While not specifically Information Operations, both of these topics are identified in Joint Pub 3-13 as Information Operations related tasks. For a subject matter that has as much emphasis as Information Operations does, the amount of instruction covered doesn't even scratch the surface of what officers need to know to effectively utilize Information Operations across the spectrum of military operations.

The primary mechanism for inclusion of an Information Operations based course in CGSOC is through an elective. This elective is mandatory for all FA30 officers attending GCSOC, but is open to all U.S. officers regardless of branch or specialty. However, it is a class that is taught at the Top Secret Special Compartmented Information (TS/SCI) level of access. It is authored by the Information Operations staff proponent located in the DJMO department within the faculty of the Command and General Staff School (CGSS) and is only offered four times during the elective phase of CGSOC. This means that only sixty out of the more than one thousand officers attending CGSOC actually get to participate in this elective, leaving the vast majority of officers attending CGSOC with no real Information Operations instruction.

The overall structure of CGSOC will change in FY2004 as the Army introduces its new Intermediate Level Education (ILE) program.[23] As the curriculum changes there will be additional training included in the program of instruction (POI) on Information Operations. Additionally, starting in AY 2003 all officers attending CGSOC will receive

[23] Intermediate Level Education is the restructuring of the CGSOC that will separate CGSOC into two segments, the core curriculum and the Advance Warfighter Application; it will begin in AY2003-2004 at Ft. Leavenworth.

an initial two-hour overview class on Information Operations along with an additional six hours of Information Operations specific instruction included within the campaign-planning portion of the CGSOC course. [24] This change to manner in which Information Operations are taught is very significant. It will be the first instance that the author can find of including a significant amount of Information Operations instruction early in a course, and also imbedded in the core instruction. This early imbedding, coupled with the continuation of the Information Operations elective, will be a step in the right direction in regards to Information Operations instruction.

The next course that is offered to Officers within the OES is the Advanced Military Studies Program (AMSP), which is taught at the School for Advance Military Studies (SAMS), Fort Leavenworth, Kansas. SAMS is a school that falls under the purview of the United States Army Command and General Staff College (USACGSC). AMSP is a voluntary follow on course that provides approximately 80 students the opportunity to study Operational Art, train to be Corps and Division planners and receive a Masters Degree in Military Arts and Sciences. The AMSP class is made up of predominantly U.S. Army officers, but there are students from each of the sister services and some Allies nations as well. Upon graduation each of the U.S. Army Officers will be assigned to a position as a Corps or Division planner.[25]

The current AMSP curriculum can be broken down into three distinct areas: history, theory and doctrine.[26] To examine how, if at all, Information Operations is

---

[24] Interview conducted with LtCol Rich Snyder, Information Operations course author for United States Army Command & General Staff College, Ft. Leavenworth, Ks. February 2003.

[25] SAMS public web site, http://www-cgsc.army.mil/sams/index.asp

[26] This statement was made by Bill Gregor, PhD a member of the SAMS faculty to the AOASF class during an overview of the AMSP curriculum during March of 2003

integrated into the current AMSP curriculum the author interviewed three civilian faculty members responsible for each of these areas.[27] Four questions were posed to each of the faculty: 1) What do see as the place for Information Operations in the AMSP curriculum? 2) What do you do in the course work you design to support it? 3) Where do you see the integration of Information Operations into AMSP happening? i.e. (history, theory, or doctrine) and 4) What is the best way to integrate the concepts of Information Operations into AMSP? While all three-faculty members saw a place for Information Operations in the curriculum of the AMSP course, there was no universal position on where it should be integrated or how that integration should occur. The consensus of the three faculty members was that while numerous elements of Information Operations were addressed in the assigned readings and class discussions, there was no effort made to build an awareness of Information Operations amongst the students.

There will be four days of Information Operations included in the AMSP program during the last phase of the AY03 course.[28] This instruction will focus on technical issues like communications bandwidth usage, then proceed to focused readings on Network Centric Warfare, and end with a practical exercise. While this four day POI will give the AMSP students some exposure to the concept of Information Operations it is too little to late. There has been no Information Operations doctrine, theory or history covered in AMSP. The students will be introduced to Information Operations concepts and issues with zero grounding in Joint, U.S. Army or Sister Service doctrine of Information Operations. It will be another example of Information Operations being

[27] On 19 and 20 March the author interviewed SAMS faculty members PhDs Robert Epstein, Bill Gregor, & Jim Schneider reference current inclusion of Information Operations within the curriculum in AMSP.

[28] AMSP course calendar for March 2003

treated as a stand-alone piece of operations and not an integrated part of operations as is stated in FM 3.0 *Operations*.[29]

There have been earlier attempts by the faculty of SAMS to introduce some Information Operations into the SAMS curriculum. During the month of January students enrolled in the AMSP program spend the month taking elective classes. During AY 2002-2003 an elective on Network Centric Warfare was offered to the AMSP students. The class was ready for presentation but cancelled due to alack of interest by the AMSP students. This would have been the first specifically Information Operations related class taught at AMSP since 1995. In 1995 SAMS taught a course titled AMSP Course 5 Information Warfare. The course material was prepared for SAMS by the Electronic Warfare Computer Applications Department of the U.S. Navy, Naval Postgraduate School (NPS), Monterey, California. The course was focused on the application of Command and Control Warfare (C2W) and numerous technological items. These items included topics like layered data networks, neural networks and optical computing.[30] While these topics are appropriate for someone studying C2W at the NPS they are not topics that need to be taught to future Corps and Division planners.

As far as the author can assess there has never been, nor is there now, an attempt to integrate Information Operations into the curriculum at AMSP. The current plan to include four days in AY 2002-2003, coupled with the past failed attempts to teach

---

[29] Department of the Army, FM 3.0. *Operations*, (Washington , D.C. Government Printing Office [GPO] 14 June 2001), 6-3.

[30] AMSP course 5 Information Warfare, Prepared by Electronic Warfare Curriculum Directorate, Naval Postgraduate School, Monterey California, 1995. p. i –iii.

Information Operations are a definite shortcoming in the curriculum at AMSP. Later in the paper a recommendations will be put forth as to how to correct this problem.

Within SAMS there is a Senior Service College (SSC) equivalent course called the Advanced Operational Art Studies Fellowship (AOASF). The Advanced Operational Art Studies Fellowship (AOASF) is the capstone program of the School of Advanced Military Studies (SAMS). Focused at the operational and strategic levels of war, AOASF is a two-year SSC-level course that prepares senior officers for colonel-level command and for operational planning assignments to within combatant and service component commands. During year one, fellows follow a curriculum that includes graduate-level study of military art and science, visits to combatant and service component commands, guest speakers, and practical exercises in campaign and major operations planning. Graduates of AOASF earn a masters degree in Military Arts and Sciences and receive Military Education code 1 (War College level graduate) credit. During year two, fellows serve as faculty members of the Command and General Staff College with particular service as seminar leaders in the Advanced Military Studies Program. [31]

As a member of the Academic Year 2003-03 AOASF class the author will assess how Information Operations has been integrated into the curriculum of AOASF. At this point the current AOASF class is eight months into an eleven-month curriculum and has yet to even discuss Information Operations. There have been no readings or class discussions about either Joint or U.S. Army doctrine for Information Operations. None of the practical application exercises have included an Information Operations

[31] SAMS public Web site, http://www-cgsc.army.mil/sams/aoasf/

component. In short the curriculum for AOASF has totally ignored the topic of Information Operations.

The United States Army War College (AWC) is the primary Senior Service College for the United Sates Army. The AWC has made significant strides in trying to include Information Operation as a part of its curriculum. In AY 2002-2003 the AWC introduced a sixty-hour elective track for Information Operations.[32] The elective track would consist of four separate modules: the first module dealing with National and Strategic Information Operations, the second module addressing DOD and Joint/ Sister Services Information Operations, the third module dealing with planning and executing Information Operations and the fourth module titled transformation and Information Operations. The elective would be a mixture of contemporary and doctrinal readings, class discussions, student presentations and guest lectures from prominent individuals who have either published works on Information Operations or leaders of military organizations involved in Information Operations planning and execution. Along with these classes at the AWC the elective will also include a trip to an Information Operations related military organization.[33] This attempt by the AWC to integrated Information Operations into its curriculum is by far the most comprehensive attempt that the author has discovered. While not perfect the AWC is taking a large step in the right direction.

[32] COL Ramos is UASWC IO integrator at Carlisle and is tasked with integrating Information Operations in the USAWC curriculum.

[33] Slide from COL Ramos' Information Operations elective Draft brief received by the author in December 2002.

The last piece of the education system that will be reviewed is that of educating/training FA30 officers. Under the current OES an FA30 officer is Military Education Level 4 (MEL4) qualified by attending and graduating from two schools. He or she must complete CGSOC in residence or by a non-resident means, and by completing a FA30 certification course taught at Fort Leavenworth. In addition to the two-week resident certification course officers must complete an on-line self-paced introduction to Information Operations course prior to coming to Ft. Leavenworth. The goal of the FA 30 Qualification Course is to provide the education and training necessary to successfully perform Information Operations officer responsibilities and functions in support of the commander at the tactical and operational levels of war in a wide variety of Army and Joint organizations. The accomplished FA 30 officer will provide offensive and defensive Information Operations integration skills to contribute to information superiority by protecting friendly information and information systems while influencing neutral and adversary information and information systems.[34] This course is a prerequisite for all FA 30 officers prior to being assigned to an FA30 duty position. The online portion of the FA30 certification course is an eighty-hour programmed instruction that is focused in two main areas. First it gives the student an overview of current Army, Navy and Air Force doctrine for Information Operations. The remainder of the course is a detailed introduction to each of the elements of Information Operations. The student must pass two quizzes and a final exam to get credit for passing this phase of the certification course.[35] The resident phase of the FA30 certification course lasts three

[34]FA30 Collaboration Site, https://www.perscom.army.mil/opfamio/fa%2030/FA30training.htm

[35] Distance Learning Course Syllabus, accessed via the AKO collaboration center for Information Operations Proponent Office.

weeks and is taught at Fort Leavenworth, Ks. This course is broken into four distinct parts. The first part is a review of the elements of Information Operations.

The next phase involves the role of these elements Information Operation in the Military Decision Making Process (MDMP). There are practical exercises that take the student through the MDMP process with an emphasis on how Information operations apply in each phase of the process. One of the strengths of the series of practical exercises is that they cover numerous military scenarios. These scenarios include Peacekeeping Operations, Non Combatant Evacuation Operations (NEO), Homeland Security Operations and High Intensity Conflict. The course is also interspersed with guest speakers from organizations or offices who have a role in supporting Information Operations. Some of theses guest lecturers include an overview from The Army Space and Missile Defense Command, a threat brief from The World Class OPFOR of BCTP, a brief from the Battle Command Battle Lab and an overview briefing from The First Information Operations Command.

As with the online portion of the course the students are evaluated during this phase of the course. Each student must pass two examinations to successfully complete this phase of the course. Along with these examinations the students are also evaluated on their ability to provide written estimates as well as their ability to write an Information Operations Annex and Estimate.[36]

Under the new ILE structure that the Army is adopting, FA30 officers will no longer attend resident CGSOC with officers from the Operations career field. They will

---

[36] Information Operations Resident Course Syllabus June 2003, accessed via the AKO collaboration center for the Information Operations Proponent Office.

attend a 3-month core course taught at a satellite campus and then complete their FA30 qualification course to receive their MEL4 qualification. This will not only eliminate FA30 officers from the one-year resident course taught at Ft. Leavenworth, but also make it very difficult for any FA30 officer to attend the AMSP course as well.

It is at these two schools where U.S. Army Majors learn how to function on higher level planning staffs. When FA30 officers no longer attend CGSOC, a critical element will be missing for both the FA30 officers and those officers in the Operations career field. The usual exchange of ideas and understanding of what each officer brings to a planning staff will be absent. The officers in the Operations career field will not get the necessary exposure to what the FA30 officer can add to a planning staff. Conversely, the FA30 officer will not be exposed to what is expected of him by the officers in the Operations career field who will make up the planning staffs upon which he will be serving.

This also applies in a similar manner to the AMSP program. If FA30 officers do not attend AMSP, there will be a lack of Information Operations officers in the career field who have been educated at the operational level of war. Additionally, the members of the AMSP seminars will not understand what an FA30 officer can add as an operational level planner, nor will the FA30 officers have the necessary exposure to what the future planners will expect from an FA30 officer.

CHAPTER FOUR

Recommendations

The following recommendations for how Information Operations should be addressed in the education of Army Officers will primarily be focused on the schools previously discussed in this monograph. These schools are CAS3, CGSOC, the FA30 certification course, AMSP, the AWC and the AOASF Fellowship. As the author is currently attending the AOASF course and will be a small group facilitator for the AMSP course next year the author will be much more detailed in my recommendations for those two courses.

Interestingly enough, with the exception of the AWC, all of these schools are located here at Fort Leavenworth and have no coordination between them as how best to educate officers in Information Operations. While each course is oriented to teaching a different level of Army Officer, there should be some coordination between the schools to ensure that Information Operations is taught consistently throughout each of them. The author assesses that this mission could be performed by the Information Operations proponent office also located at Ft. Leavenworth. The author would give them the mission of reviewing the curriculum at each of these schools and ensuring that Information operations are addressed in each school, and that what is taught is consistent and nested throughout each course. By doing this you would be able to educate Army officers from the rank of Captain through Colonel with a consistent and integrated understanding of Information Operations.

The first Army school where Information Operations needs to be part of the curriculum is at CAS3. The reason that Information Operations needs to be taught here is

that CAS3 is the first time that officers of all branches are mixed together and go through the Military Decision Making Process (MDMP) as a group. This group of combat arms, combat support and combat service support arms replicates what officers are likely to experience once they are part of a planning staff. The author believes that it was a mistake to eliminate the Information Operations block from the CAS3 curriculum. It is the author's assessment that the best way for CAS3 to integrate Information Operations back into the curriculum is by using the same framework they used before. They should an Information Operations estimate as part of the course objectives for each military operation that they plan. By having the students conduct an Information Operations estimate for each operation they conduct they will begin to see Information Operations as an integrated part of every military plan. By including the Information Operations estimate along with the Logistics and Intelligence estimates it reinforces the idea that Information Operations are part of every plan and not some piece that gets added on as an afterthought.

The next school addressed is the resident CGSOC. The core course that all students were taught had almost no Information Operations as part of the curriculum. While there is a very informative and well-organized elective that is taught it is just that, an elective. As an elective it only is taught to fraction of the CGSOC class. By teaching Information Operations as an elective it only continues to perpetuate the belief that Information Operations are not a necessary part of any plan but are something that gets included at the end of the plan as an afterthought. It is this perception that Information Operations are not a necessary part of every military plan that has to be overcome. The way that this should be accomplished at CGSOC is similar to the way that it should be

done at CAS3. Information Operations should be addressed early in the CGSOC course and taught to all students as an integrated part of their tactics instruction. Much like was previously discussed with CAS3 this would ensure that Information Operations were included as part of the estimate processes that would be done by each staff group and student.

The United States Army War College (AWC) has the most extensive program for including Information Operations into their curriculum. As noted earlier they have an Information Operations elective track that runs throughout the second and third terms of their course. While this program is extensive, it has the same shortcoming as the current CGSOC Information Operations education. That shortcoming is the fact that it still addresses Information Operations as an elective course or track and not as a common core course. No matter how good an elective is, it is always just an elective. The AWC needs to do the same thing that the author recommended for CGSOC when it comes to educating all officers in Information operations. They need to ensure that all officers attending the AWC get a thorough doctrinal overview during their first term. This will ensure that they have a grounding in the principles and elements of information operations that they can apply throughout the year.

The AWC can keep the Information Operations elective track and use it as a more advanced course of study for those officers who have a need or desire for further study.

The final course addressed is the AMSP. As the school that produces future Corps and Division planners, and administers to the AOASF program that produces future operational and strategic planners, it is imperative that the School of Advanced Military Studies fully incorporate Information Operations into its curriculum. The fact that

Information Operations is currently ignored in both the AMSP and the AOASF curriculum is a deficiency that has to be addressed. As the emphasis placed on Information Operations continues to increase there is no better place in the Army to accomplish this task than at SAMS.

In the case of both the AMSP course and the AOASF fellowship it is imperative that a basic understanding of Information Operations be established early in the class schedule. The reason for this early understanding is so that each student can have a basic frame of reference from which to operate. Using this baseline understanding students will then be able to apply this doctrine both to historical examples as well as to practical exercises that are conducted throughout the year.

For the AMSP students this basic understanding can be attained in one of two ways. The first way that this could be accomplished would be by dedicating a week of class early within the AMSP curriculum to an overview of Information Operations. This week of class would begin with an overview of current Information Operations doctrine within the United States military. Each seminar, which consists of fourteen officers, would be divided into four groups. One group would review current U.S. Army doctrine, the second would review current U.S. Air Force doctrine, the third group would review current Navy doctrine, and the last group would review current Marine Corps doctrine. Each of the groups would also review current Joint Doctrine for Information Operations. The purpose of these readings would be to establish a basic understanding of Information Operations and to allow each group to understand how the individual services plan to focus their efforts.

The next step would be to look at three examples of military campaigns and assess how the current doctrinal elements of Information Operations were addressed in each campaign. The three campaigns that the author would choose would be a World War II scenario, Operation Desert Shield/ Desert Storm, and Iraqi Freedom. Depending on which campaigns are used, elements like Computer Network Attack (CNA) and Computer Network Defense (CND) will not be applicable. However, the absence of these two elements doesn't make a campaign any less relevant for study.

The intent of looking at these campaigns is two fold. First is to show that Information Operations is not a totally new concept. That most, if not all, of the elements that we now consider part of Information Operations has been part of successful military planning for quite some time. Secondly is to show that Information Operations is not only about computers and computer systems. While these elements get most of the attention, they make up only a small part within the larger concept of Information Operations.

The second way that AMSP students could receive a basic understanding of Information Operations is through the addition of a mandatory CGSC prerequisite. By requiring AMSP applicants to take the Information Operations elective at CGSC each AMSP student would begin their year at SAMS with a basic understanding of Information Operations. While this would require some prior planning and coordination with the CGSOC faculty the concept already exists. Currently, each CGSOC student who will attend AMSP takes A699 Classical Theorists as a mandatory prerequisite for attendance to AMSP.

Each of these solutions will ensure that the AMSP student will have a working understanding of Information Operations doctrine prior to the start of AMSP.

The AOASF curriculum for 2003-2004 has not included any readings, discussions, or practical exercises dealing with Information Operations. A review of next years proposed curriculum does include a week, which will focus on Information Operations. The current schedule places this week in the February/ March Time frame. It will include a one-day review of the German Blitz of France in 1941, a day dedicated an overview current Information Operations doctrine, and two days of a practical exercise.[37] While the mere inclusion of some Information Operations topics is an improvement there are some flaws with the way it is being addressed. First it is being included too late in the year. As was stated earlier Information Operations needs to be included early in the course so all the students have a basic understanding of Information Operations. A block of instruction on Information Operations should be included within the first third of the class schedule. This will enable the AOASF students to apply the basic principles of Information Operations

As part of the AOASF curriculum the fellowship makes two trips to Washington D.C. during the first third of the schedule.[38] During one of these trips to Washington D.C. the author recommends that a day be added to one of the trips so that the AOASF fellows can visit the 1st Information Operations Command (1stIOCmd) (Land) that is located at Fort Belvoir. This command was formally titled the Land Information Warfare Activity (LIWA) and is the Army's only command, which focuses entirely on

[37] AY2003-2004 propose AOASF class schedule produced by AOASF Director, Peter Schifferle, PhD.

[38] This information was derived from the proposed AY 2003-04 schedule that has been produced by the AOASF Director, Pete Schifferle.

Information Operations. The mission of 1stIOCmd is to provide Information Operations support to the Army by supporting the warfighter in planning, synchronizing and executing Information Operations for the commander.[39] A one day visit to 1stIOCmd would give the Fellows an overview of what this command is responsible for, as well as what support they might be able to receive from 1stIOCmd as a strategic level planner.

If it is not feasible for the fellows to visit Ft. Belvoir then it is the author's recommendation that SAMS have a representative from 1stIOCmd come and brief the fellows here at Fort Leavenworth. This alternative would be very easy to set up. During the FA30 certification course taught here at Ft. Leavenworth a overview brief by the 1st IOCmd is included as part of the normal class schedule. With very little coordination, the faculty at SAMS could get the presenter to either give the Fellows this same brief or get a briefing tailored to their needs as future strategic and operational planners. It would also be a good idea to have the AMSP students receive at least the overview of 1stIOCmd that the FA30 officers receive. This would help with their understanding of Information Operations, and also expose them to the assistance they could expect from 1stIOCmd as Corps and Division planners.

My final recommendation involves the way that FA30 officers are going to be trained as we move to ILE. The current FA30 qualification course does a good job of initial training for new

FA30 officers. When this is coupled with a year of CGSOC these officers should be

[39] This mission statement was taken from the LIWA Command Brief available at the Information Operations Collaboration Center on Army Knowledge Online (AKO).

prepared to be competent Information Operations staff officers. It is the mix of these two courses that will be missing under the new ILE structure. Under ILE the FA30 officers will no longer come to Ft. Leavenworth with the officers of the Operations Career Field. They will attend their three-month core CGSOC at a satellite location with officers who are not in the Operations Career Field. This will have a negative impact on both the officers in Operations Career Field as well as the FA30 officers.

Officers who will have attended CGSOC in residence at Fort Leavenworth will populate the future staffs that the FA30 officers will serve on. Neither the FA30 Officer, nor the officers who make up the staff will have worked through problems as a team. Each will have received their MEL4 level education in isolation from the other. The FA30 officer will not have had the needed exposure to the thought processes of the staff officers, and the staff officers will not have had the opportunity to work through the MDMP process with an FA30 officer. Each group will be educated in a vacuum from one another. Instead of staff officers who know that information Operations need to be an integrated part of every plan they will see the FA30 officer as a someone who is a specialist and not an integral part of the planning team.

The only way to correct this problem is for the Army to reassess the way the FA30 Officers receive their MEL4 certification under ILE. It is the author recommendation of the author that all FA30 officers be sent to Fort Leavenworth for the one year CGSOC and not to a satellite campus for the non Operations Career Field 3 month course. By attending CGSOC with the officers in the Operations Career Field the FA30 officer will be seen as an integral part of the planning staff. This will also allow

the FA30 officers to work through military problems and participate in the MDMP with the officers who will make up future planning staffs.

The attendance at the one-year CGSOC at Fort Leavenworth will also make it more likely that FA30 officers can attend AMSP. Currently FA30 officers graduating from CGSOC can apply to stay on at Fort Leavenworth for AMSP. Under ILE a FA30 officer who would like to attend AMSP would have to apply and PCS to Leavenworth for a year to attend AMSP. This would mean that his current organization would have to release him to allow him to attend the program. This release and the one-year commitment as a Corps or Division planner would mean that you lose the officer. With the current high demand for FA30 officers in the field this author cannot envision organizations allowing officer to attend AMSP. However, if the attended CGSOC with the officers in the Operations Career Field this problem of needing to released by an organization would be mute.

CHAPTER FIVE

Conclusions

There are two things that are certain when it comes to Information Operations. First, information Operations are becoming an increasingly important in military operations. Secondly, the United States Army needs to do a better job of educating all its officers on this subject. Too many people think that Information Operations are a new 21st Century occurrence that is all about digitization and information technology.[40] It is in fact not some totally new 21st century phenomenon. With the exception of its three purely computer related elements, the remaining elements of Information Operations have been around for many years.

With our increased dependence on digitization and automated command and control systems, special emphasis must be placed on the integration and synchronization of Information Operations into all current military operations. To accomplish this the U.S. Army needs to include education and training on Information Operations at all levels of its OES beginning with Phase II of the Captains Career Course. This will ensure that all officers have an appreciation of what Information operations are, and that they are an integral part of all modern military operations. It is this understanding that Information Operations are a part of all military operations that is currently lacking thorough out the OES.

There are no schools in the U.S. Army where Information Operations has been fully integrated into the curriculum. In the cases of both the Army War College and the Command and General Staff College there has been some attempt to educate officers on

[40] Thaddeus A. Dmuchowski, Educating Today's Warriors on the Information Battlefield, Strategy Research Project AY00, U.S. Army War College, Carlisle Barracks, Pennsylvania. p. 14.

Information Operations. While they both have established good Information operations electives courses they are just that, electives. Both institutions lack any real Information Operations instruction in their core curriculum. Information Operations should be taught in the same manner as logistics and intelligence, as integral parts of any operation.

Of particular note is the total absence of Information Operations in both the AMSP and AOASF courses at SAMS. If SAMS is intended to produce premiere military planners for the Army, then it is inconceivable that Information Operations are ignored in the core curriculum. While AMSP has dedicated a portion of its Futures week to Information Operations it is too little too late. Addressing Information Operations during the last week a yearlong course does nothing to ensure that future planners will be able to ensure Information Operations are an integrated and synchronized part of military planning. If Information Operations are not addressed early and included as a topic of interest throughout the year we will not be making progress.

With regard to the AOASF portion of SAMS there has been no attempt to integrate Information Operations into the curriculum. While the course director has included some instruction on Information Operations in next year's curriculum it has to be done early in the year, and reinforced throughout the year, to be effective.

From Phase II of the Captains Career Course through the Senior Service College Courses, Information Operations needs to be part of each schools core curriculum. The basic rule of thumb is that if a course teaches MDMP then it needs to have Information Operations included as part of the curriculum. This will ensure that Information Operations are synchronized as part of military planning. The goal is to train officers who automatically include the elements of Information Operations into their planning

efforts. You will be able to tell when this has been accomplished when Information operations are considerations like intelligence and logistics, not some mysterious add on item as they are now. Until we do include Information operations as the author has suggested we will continue to produce officers who have no idea what Information Operations are and the benefit to be gained by including Information Operations in military plans.

The Army has done an excellent job in producing doctrine to support Information Operations. Both FM 3.0 *Operations* and FM 3-13 *Information Operations* are well-written, understandable documents that lay out a good framework for conducting Information Operations. The next step that needs to be taken is including this doctrine into our officer education courses. Until we do this you can have all the well-written doctrine in the world and it will be worthless.

The increased emphasis on Information Operations is here to stay. This point was made clear during the morning media briefings conducted by BG Vincent Brooks during "Operation Iraqi Freedom". During the first week of the campaign every opening statement included the phrase, "the Coalition Information Operations plan continues". Now all the U.S. Army must do is to teach its officers and future military planners just what that means.

APPENDIX

Elements of Information Operations

Military Deception. "Military deception includes measures designed to mislead adversaries and enemies by manipulation, distortion, or falsification. Its aim is to influence the enemy's situational understanding and lead him to act in a manner that favors friendly forces."

Counterdeception. "Counterdeception includes efforts to negate, neutralize, or diminish the effects of, or gain advantage from, a hostile deception operation. Counterdeception supports offensive IO by reducing harmful effects of enemy deception. Defensively, counterdeception identifies enemy attempts to mislead friendly forces."

Operations Security. "Operations security (OPSEC) denies the enemy information critical to the success of friendly military operations. It contributes to the security of Army forces and their ability to surprise enemies and adversaries. OPSEC identifies routine activities that may telegraph friendly intentions, operations, capabilities, or military activities. It acts to suppress, conceal, control, or eliminate these indicators. OPSEC includes countersurveillance, signal security, and information security."

Physical Security. "Physical security prevents unauthorized access to equipment, installations, and documents. It safeguards and protects information and information systems."

Electronic Warfare. "Electronic warfare (EW) is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW can cause an enemy to misinterpret the information received by his electronic systems. EW includes—"

- **Electronic attack**. "Electronic attack involves actions taken to degrade, neutralize, or destroy enemy electronic combat capabilities. Actions may include lethal attack, such as antiradiation missiles and directed energy weapons, and nonlethal electronic attack, such as jamming."
- **Electronic protection**. "Electronic protection involves actions taken to protect friendly use of the electronic spectrum by minimizing the effects of friendly or enemy EW. Actions may include radio silence and antijamming measures."
- **Electronic warfare support**. "Electronic warfare support involves detecting, identifying, locating, and exploiting enemy signal emitters. It contributes to achieving situational understanding, target development and acquisition, damage assessment, and force protection."

Information Assurance. "Information assurance protects and defends information systems. Threats to information systems include physical destruction, denial of service, capture, environmental damage, and malfunctions. Information assurance provides an enhanced degree of confidence that information and information systems possess the following characteristics: availability, integrity, authentication, confidentiality, and nonrepudiation. Computer network defense is part of this element."

Physical Destruction. "Physical destruction applies combat power against IO-related targets. Targets include information systems, EW systems, and command posts. Physical destruction that supports IO is synchronized with other aspects of the operation. For example, when deciding whether to destroy an enemy command post, the friendly commander weighs the advantages gained from disrupting enemy C2 against those gained from collecting information from the command post's radio traffic."

Psychological Operations. "Psychological operations (PSYOP) are planned operations that influence the behavior and actions of foreign audiences by conveying selected information and indicators to them. The aim of PSYOP is to create behaviors that support US national interests and the mission of the force. PSYOP are closely integrated with OPSEC, military deception, physical destruction, and EW to create a perception of reality that supports friendly objectives."

Counterpropaganda. "Counterpropaganda includes activities directed at an enemy or adversary conducting PSYOP against friendly forces. Counterpropaganda can contribute to situational understanding and expose enemy attempts to influence friendly populations and military forces. Preventive actions include propaganda awareness programs that inform US and friendly forces and friendly populations about hostile propaganda."

Counterintelligence. "Counterintelligence consists of activities that identify and counteract threats to security posed by espionage, subversion, or terrorism. It detects, neutralizes, or prevents espionage or other intelligence activities. Counterintelligence supports the commander's requirements to preserve essential security and protect the force."

Computer Network Attack. "Computer network attack consists of operations that disrupt, deny, degrade, or destroy information resident in computers and computer networks. It may also target computers and networks themselves. Although theater or national elements normally conduct computer network attack, the effects may be evident at corps and below."

Computer Network Defense. "Computer network defense consists of all measures to defend computers and other components that are interconnected in electronic

telecommunications networks against computer network attacks by an adversary. Such measures include access controls, detection of malicious computer code and programs, and tools to detect intrusions. Army forces use inherent capabilities and accomplish specific computer network defense actions to defend computer networks from unauthorized users."

Public Affairs. "Public affairs operations influence populations by transmitting information through the news media. They fulfill the Army's obligation to keep the American people and the Army informed. Public affairs help to establish conditions that lead to confidence in the Army and its readiness to conduct operations in peace, conflict, and war. Disseminating this information is desirable and consistent with security. Information disseminated through public affairs counters the effects of propaganda and misinformation."

Civil-Military Operations. "CMO applies civil affairs to military operations. It encompasses activities that commanders take to establish, maintain, influence, or exploit relations between military forces and civil authorities—both governmental and nongovernmental—and the civilian populace. Commanders direct these activities in friendly, neutral, or hostile AOs to facilitate military operations and consolidate operational objectives. Civil affairs may include performance by military forces of activities and functions normally the responsibility of local government. These activities may occur before, during, or after other military actions. They may also occur as stand-alone operations. CMO is the decisive and timely application of planned activities that enhance the relationship between military forces and civilian authorities and population. They promote the development of favorable emotions, attitudes, or behavior in neutral, friendly, or hostile groups. CMO range from support to combat operations to assisting countries in establishing political, economic, and social stability."

BIBLIOGRAPHY

Advanced Operational Arts and Studies Fellowship (AOASF) Mission Statement, United States Army Command & General Staff College, Ft. Leavenworth, Kansas. https://www-cgsc.army.mil/sams/aoasf/ accessed 3 February 2003.

Alberts, Gartska, and Stein. Network Centric Warfare. Washington D.C.: DoD Command and Control Research Program, 1999.

Corps and Division Operations (F646), Lesson plan from Combined Arms and Services Staff School, 1998.

Dmuchowski, Thaddeus A. Educating Today's Warriors on the Information Battlefield, May 2003, U.S. Army War College, Carlisle Barracks, Pennsylvania.

Epstein, Robert, U.S. Army, interviewed by LTC Tom Gregory, January 2003, United States Army Command & General Staff College, Ft. Leavenworth, Kansas.

Eassa, Charles N. US Armed Forces Information Operations-Is the Doctrine Adequate. School of Advanced Military Studies, USACGSC, Ft. Leavenworth Ks. First Term AY 99-00.

Functional Area 30 Training Overview web site, United States Army Command Arms Center, Ft. Leavenworth, Kansas. Internet, https://www.perscom.army.mil/opfamio/fa%2030/FA30training accessed 15 March 2003.

Gregor, William, interviewed by LTC Tom Gregory, March 2003, The School of Advanced Military Studies, Ft. Leavenworth, Kansas.

Land Information Warfare Activity (LIWA) Command Briefing, HQ LIWA Fort Belvoir Virginia. Internet, https://www.us.army.mil/portal/jhtml/community.jhtml?cpid Accessed 15 March 2003.

Layton, Joseph MAJ (P), U.S. Army, interviewed by LTC Tom Gregory, January 2003, United States Army Command & General Staff College, Ft. Leavenworth, Kansas.

Information Warfare, AMSP Course 5, School of Advanced Military Studies, United States Army Command & General Staff College, Ft. Leavenworth, Kansas, 5 June 1995.

Operation Bosanova After Action Review, accessed granted by the Office of the SFOR Command Historian via the SFOR NATO Restricted LAN, in Sarajevo, Bosnia Herzegovina, January 26 2003.

Ramos, Felix, COL U.S. Army, Draft Information Operations Elective Track for AY03 Brief, U.S. Army War College, Carlisle Barracks, Pennsylvania.

School of Advanced Military Studies Public Web Site, overview of SAMS, Internet, http://www-cgsc.army.mil/sams/index.asp
Accessed 11 March 2003.

Schneider, James J. Interviewed by LTC Tom Gregory, January 2003, United States Army Command & General Staff College, Ft. Leavenworth, Kansas.

Snyder, Rich LtCol, U.S. Air Force, interviewed by LTC Tom Gregory, January 2003, United States Army Command & General Staff College, Ft. Leavenworth, Kansas.

Sun Tzu, *The Art of War.* Translated by Samuel B. Griffin. New York: Oxford University Press, 1963.

TRADOC PAM 525-5, Force XXI Operations 1 August 1994, Headquarters, United States Army Training and Doctrine Command, Fort Monroe, Virginia.

Turabian, Kate L. *A Manual for Writers of Term Papers, Theses, and Dissertations.* 6th ed. Chicago: University of Chicago Press, 1996.

United States Department of Defense. Joint Vision 2010. Washington D.C.: U.S. Government Printing Office, 1 Sep 2001.

United States Department of the Army. FM 3.0 *Operations.* Washington D.C.: Office of the Chief of Staff of the Army, June 2001.

United States Department of the Army. FM 3-13 *Information Operations.* Washington D.C.: Office of the Chief of Staff of the Army, Draft Regulation.

United States Department of the Army. FM 100-6 *Information Operations.* Washington D.C.: Office of the Chief of Staff of the Army, August 1996.